BACKGROUND OF INVESTIGATION

1) Your Affiant knows from training and experience that computer users can install publicly available software that accesses a network known as *Freenet. Freenet* is a distributed, Internet based, peer-to-peer network which lets a user anonymously share files and chat on forums. *Freenet* is free software and the source code is publicly available. Communications between computers running *Freenet*, or nodes, are encrypted and routed through other *Freenet* nodes making it difficult to determine who is requesting the information and what the content is of the information being requested. *Freenet* provides a platform for message forums and *Freesites*, websites only available through *Freenet*.

2) Your Affiant knows from training and experience that files, or parts of files, are stored in *Freenet* using a key created from a compressed digital representation method called Secure Hash Algorithm Version 256 or SHA256.

3) Your Affiant knows from training and experience that *Freenet* breaks a file into small pieces, or blocks, each with their own unique key based on this SHA256 value. These small blocks are then distributed across *Freenet* users, or nodes, and stored in disk space provided by each user to *Freenet*. No one user has the entire intact file. The keys to all of the parts of a file are found in a high level index block, or manifest.

4) Your Affiant knows from training and experience that Internet computers identify each other by an Internet Protocol or IP address. Your Affiant knows that these IP addresses can assist law enforcement in finding the location of a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

5) Your Affiant knows from training and experience that a computer running *Freenet* will receive requests from other computers running *Freenet* containing the key of a part of a file to retrieve from that node's data store, or to forward to another user that may have that part of the file.

6) Your Affiant knows from training and experience that *Freenet's* attempt to hide what a user is requesting from the network has attracted persons that wish to collect and/or share child pornography files. Freenet is not a significant source of music, adult pornography, theatrical movies or other copyright material.

7) Your Affiant knows from training and experience that *Freenet* users connect to other users, unknown to them, or peers. They then send requests to these peers for the blocks of files they are attempting to download.

8) Your Affiant knows from training and experience that the requests that a user of *Freenet* sends to a peer contain only the key for the block of data and not the encryption password to make the data readable. A user relies on the inability of a peer to decrypt a block of data or know what file contains this block to hide his use of the *Freenet* network to obtain child pornography files.

9) Your Affiant knows from training and experience that someone requesting blocks of a file has taken substantial steps to install *Freenet* and locate a file's key to download. *Freenet* provides no search mechanism common to other file sharing systems. A subject desiring to download a file must first find the key on a *Freesite* or message board containing material of interest.

10) In September 2011, law enforcement officers began an undercover operation collecting keys and files being publicly shared on *Freenet*, in order to build a data base of keys associated with known or suspected child pornography.

11) In April 2012, law enforcement officers began running copies of *Freenet* that had been modified for law enforcement to log the IP address, key, and date and time of requests that were sent to these law enforcement *Freenet* nodes. These keys are then compared to keys of known child pornography to identify IP addresses soliciting child pornography.

12) Your Affiant knows from training and experience that streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of the file.

13) Your Affiant knows from training and experience that over fifty (50) search warrants or consent searches have been conducted in the United States and Canada by using the above method of investigation. This method has proven to be reliable in determining the location of computers that were involved in using *Freenet* to obtain child pornography. By using the above method of investigation, nearly every case was verified through the following means:

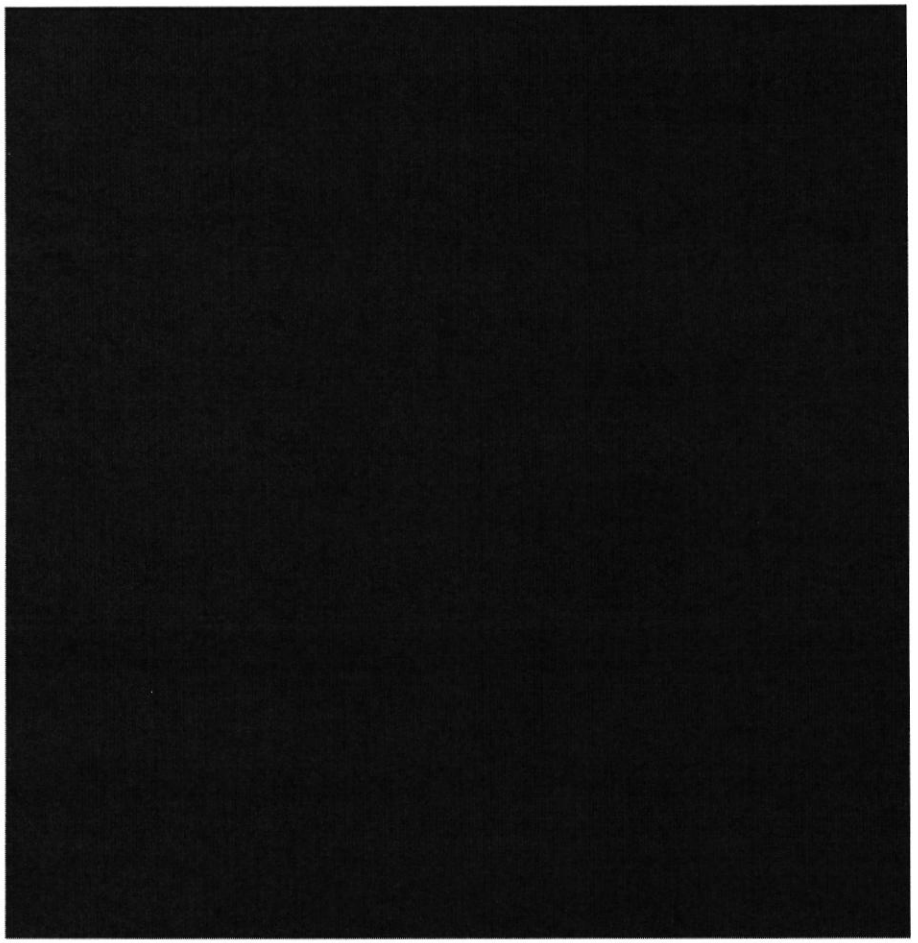
1). Evidence of child pornography was found on the computer(s) or other media.

2.) Interviews of persons using those computers verified that child pornography had been present at one time but had been deleted or the computer with the child pornography had been removed from the premises.

3.) Evidence of the use of encryption software to hide files was found on the computer.

SPECIFIC PROBABLE CAUSE

[redacted]



SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

1) Your Affiant knows from training and experience that searches and seizures of evidence from computers and other Internet access devices require law enforcement agents to seize most or all electronic items (hardware, software, passwords, and instructions) at the specified premises, to be analyzed later by a qualified digital evidence specialist in a controlled environment. Digital storage media may include but is not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks, or other magnetic, optical, or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data or images of child pornography, which can store the equivalent of thousands of pages of information. Users may store information or images in random

order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is evidence included in the scope of the search warrant. This sorting process renders it impractical to attempt this kind of data search on site.

2) Your Affiant knows from training and experience that searching digital storage systems for evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, and/or encrypted files. Since digital evidence is vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

3) Your Affiant knows that if computers, or other digital devices, are found in a running state the contents of volatile memory, the use of encryption, or the use of other communications devices, such as routers, make it necessary to gather evidence from these devices at the site.

4) Your Affiant knows from training and experience that persons trading in, receiving, distributing or possessing images involving the exploitation of children, or those interested in the actual exploitation of children, often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images and/or provide evidence of a person's interest in child pornography.

5) Your Affiant knows from training and experience that child pornography files found on computers and other digital communications devices are usually obtained from the Internet or from cellular data networks using application software which often leaves files, logs, or file remnants which would tend to show the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files.

6) Your Affiant knows from training and experience that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

7) Your Affiant knows from training and experience that computers or other digital devices used to access the Internet and store digital files can be small and portable and may be found on persons and in vehicles and other out buildings on a premise.

8) Your Affiant knows from training and experience that digital crime scenes usually include items or digital information that would tend to establish ownership or use of digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts to participate in the exchange, receipt, possession, collection, or distribution of child pornography.
IS
9) Your Affiant knows from training and experience that searches of premises involved in computer, or digitally related, criminal activity usually result in the location of items that tend to establish ownership or use of digital devices, and ownership or use of Internet service accounts accessed to obtain child pornography, to include credit card bills, telephone bills, correspondence, and other

identification documents.

10) Your Affiant knows from training and experience that search warrants of premises usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, and other identification documents.

11) The statements contained in this affidavit are based on this affiant's personal knowledge and information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to this affiant concerning this investigation.

DEFINITIONS USED IN THIS AFFIDAVIT

1) Internet Protocol (IP) address
   An IP version 4 (IPv4) address is a 32-bit number that uniquely identifies a host connected to the Internet. An IP address is expressed in "dotted decimal" format, consisting of the decimal value (0-255) of its four bytes, separated with periods; an example IPv4 address is 207.32.187.12. IP version 6 (IPv6) addresses are 128 bits in length.
2) Node
   A computer on the Internet running the *Freenet* software.
3) Manifest
   The highest level record in *Freenet*. It is pointed to by the manifest key and contains keys, or pointers to keys, for the blocks of the file. It also includes metadata about the file such as its size, hash values, and compression. May contain the entire file if it is less than 32kb.
4) Key
   One of the types of values used on *Freenet* to reference file manifests, blocks, or web pages.
5) Block or Split
   A 32KB block of data that makes up a file. These are referenced with the SHA256 hash of the block.
6) Freesite
   A website within *Freenet*. Only accessible using the *Freenet* interface.
7) Darkweb or Deepweb
   Terms to describe networks and Internet use that is not obvious or accessible by the causal user. Most P2P and anonymous networks fall into this category.
8) Datastore
   The disk storage contributed to Freenet to store data blocks. This storage is used by the Freenet network and does not contain user data.
9) SHA1, SHA256
   SHA1 AND SHA256 are part of a set of cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). Cryptographic hash functions are a kind of algorithm or mathematical operation run on digital data, and by comparing the result (hash) of the execution of the algorithm to a known and expected hash value, a person can determine the data's authenticity. An example is running a hash on downloaded software and comparing the result to the developer's published hash result, to see if the software is

genuine, and safe to run. Peer-to-peer file sharing systems use these values to assure the contents of files.

10) Peer-to-peer (P2P)

A distributed network architecture whereby network hosts share their resources (such as processing power and storage capacity) with other hosts without the need for a central managing device. Most Internet applications are *client-server*, whereby a host (e.g., an e-mail or Web user) obtains a service from another host (e.g., an e-mail or Web server). In a P2P environment, hosts communicate directly without the need of a server.